REMARKS

Reconsideration of the above-identified application in view of the amendments above and the remarks following is respectfully requested.

Claims 1-146 are in this Application. Claims 81-106 and 131-146 have been withdrawn from consideration. Claims 1-75 and 78-130 have been rejected under 35 U.S.C. §102. Claims 76 and 77 have been rejected under 35 U.S.C. §103. Claims 1, 73, 107, and 110 have been amended herewith. New claims 147 and 148 have been added herewith.

35 U.S.C. §102 Rejections

Claims 1-72 and 110-129 are rejected under 35 U.S.C. §102(b) as being anticipated by Ginter et al. (US Patent No. 5,892,900), hereinafter "Ginter".

Claims 73-75, 78-80 and 130 are rejected under 35 U.S.C. §102(b) as being anticipated by Ronning (US Patent No. 5,903,647), hereinafter "Ronning".

Claims 107-109 are rejected under 35 U.S.C. §102(b) as being anticipated by "Java Security: How to Install the Security Manager and Customize Your Security Policy" (hereinafter "Venners".)

I. Rejections in light of Ginter

The Examiner rejected claims 1-72 and 110-129 under 35 U.S.C. §102(b) as being anticipated by Ginter et al.

Claims 1 and 110 are hereby amended to include performing a statistical analysis upon the content in use by the user. The statistical analysis determines whether this content includes any confidential information for which a security policy has been defined. If so, the user's actions are controlled as required by the security policy.

Amended claim 1 states:

> 1. A method for computer workstation based information protection, the method comprising:
>
> a) monitoring a user's actions on said computer workstation,
>
> b) *performing a statistical analysis of content in use by said user to identify confidential information in said content,*
>
> c) analyzing said actions with respect to *a pre-defined policy associated with said identified confidential information*, to determine whether said actions prejudice said confidential information, and
>
> c) executing said policy in accordance with the results of said analysis to control said actions. (Emphasis added.)

A corresponding amendment is made to claim 110.

The present method associates a security policy with the confidential information itself, rather than with documents (or other content) containing a specific instance of the information. For example, the same confidential information may appear in a MS-Word file, a PDF file, a spreadsheet and an email message. Additionally, the information may be accessed by (or from) different servers, desktop computers and/or laptop computers. By providing a policy for the confidential information itself, it becomes unnecessary to define a separate policy for each of its instances.

Once the policy is provided, users' actions on the confidential information, regardless of the information's format or location, are analyzed to determine whether they prejudice the confidential information. The security policy is executed in accordance with the results of the analysis in order to control the user's actions.

Statistical identification of the confidential information, together with other claim limitations, constitutes, technically and conceptually, a novel and inventive method for protecting confidential information on computer workstations.

Support for the above amendments is found in para. 0313 of the instant specification which states:

> In a preferred embodiment of the present invention, the client is operable to detect confidential information, based on statistical identifiers resides in a specialized database. In a preferred embodiment of the present invention, the specialized database resides on a secure server. FIG. 6 illustrates a system, substantially similar to the system of FIG. 1, where a content identifier 180 is used in order to identify the content, possibly using the information stored in the content identifier database 182. The results of the identification process are transferred to the policy reference monitor 132, possibly with an accompanying "confidence level" that represents the amount of uncertainty in the identification. The policy reference monitor 132 determines the policy that need to be applied with respect to the identified content and instructs the policy enforcement component 134 accordingly.

Ginter does not perform a statistical analysis of the content upon which the user is working to identify confidential information. In Ginter electronic documents are "placed" by the organization in virtual containers. The containers are associated with security policies that are applied to documents within the containers. These containers form a type of meta-data associated with the document, which indicates whether and how actions upon the document should be controlled. Thus in Ginter the security policy is applied to the document, and not to statistically-identified confidential information within the document.

Claims 1 and 110 are further amended to replace the limitation of "prevent or modify or restrict or monitor or log said actions" with the term "control said actions". Applicant respectfully submits that claims 1 and 110 are broadened by said amendment.

It is therefore respectfully submitted that independent claims 1 and 110 are both novel and inventive over the cited prior art.

It is believed that the dependent claims 2-72 and 111-129 are allowable as being dependent on allowable main claims. The specific objections against the dependent claims are therefore not responded to individually.

II. Rejections in light of Ronning

The Examiner rejected claims 73-75, 78-80 and 130 under 35 U.S.C. §102(b) as being anticipated by Ronning.

Claim 73 is hereby amended to include performing statistical analysis of the content in use, to identify confidential information items for which a protection policy has been defined. Claim 73 states:

> 73. A method for information protection, said information comprising information items, said information being for usage on a computer workstation, comprising:
>
> a) defining an information protection policy with respect to an information item,
>
> b) determining the measures required to protect said information item according to said policy,
>
> c) *performing a statistical analysis of content in use on said computer workstation to identify said information item*, and
>
> d) allowing said usage on a computer workstation of content comprising said information item only while said required measures are being applied.

A corresponding amendment is made to claim 130. Support for the amendments of claims 73 and 130 is found in para. 0313 of the instant specification, as presented for claim 1 above.

Ronning relates to protecting the distribution of digital material, by providing the distributed information with an accompanying usage file. The usage file dictates how the distributed instance (i.e. the distributed file or program) is to be used. Applicants respectfully believe that Ronning does not perform a statistical analysis of the digital material to identify confidential information therein.

It is therefore respectfully submitted that independent claims 73 and 130 are both novel and inventive over the cited prior art.

It is believed that the dependent claims 74-80 are allowable as being dependent on an allowable main claim. The specific objections against the dependent claims are therefore not responded to individually.

III. Rejections in light of Venners

The Examiner rejected claims 107-109 under 35 U.S.C. §102(b) as being anticipated by Venners.

Claim 107 is hereby amended to include performing statistical analysis of the content associated with an event, to identify confidential information items for which protection is required. Claim 107 states:

> 107. A method for computer workstation based information protection, the method comprising:
> a) detecting an event occurring at said workstation,
> b) *performing a statistical analysis of content associated with said event to identify confidential information within said content*, and
> c) employing information protection based on an assessment of an importance of said event to protection of said confidential information. (Emphasis added.)

Venners relates to the operation of the Java Security Manager. The Java Security Manager is required to authorize actions judged to be potentially unsafe before the action is taken.

Applicants respectfully believe that Venners does not perform a statistical analysis of the content upon which the action is taken in order to identify confidential information therein.

It is therefore submitted that claim 107 is both novel and inventive over the cited prior art.

It is believed that the dependent claims 108 and 109 are allowable as being dependent on an allowable main claim. The specific objections against the dependent claims are therefore not responded to individually.

35 U.S.C. §103 Rejections

Claims 76 and 77 are rejected under 35 U.S.C. §103(a) as being unpatentable over Ronning as applied by the Examiner to claim 73 and further in view of England et al. (US Patent Application Publication No. 2003/0200435), hereinafter "England".

Applicants respectfully submit in response that claims 76-77 are patentable, in the light of arguments set forth below.

In order to establish obviousness, the prior art references when combined must teach or suggest all the amended claims limitations. Neither Ronning nor England teach performing a statistical analysis of content in use to identify an information item. Therefore, no prima facie case of obviousness has been established regarding the limitations of claims 76-77.

New Claims

New claims 147 and 148 have been herewith added. Claims 147 and 148 include the limitation, previously present in claims 1 and 110 respectively, that the user action is prevented, modified, restricted, monitored or logged. No new claimed limitations are added by the addition of claims 147 and 148.

No new matter has been added in the course of making the present amendments.

It is believed that all of the matters raised by the Examiner are overcome.

In view of the above amendments and remarks it is respectfully submitted that claims 1-80, 107-130, 147 and 148 are now in condition for allowance. A prompt notice of allowance is respectfully and earnestly solicited.

Respectfully submitted,

Martin D. Moynihan

Martin D. Moynihan
Registration No. 40,338

Date: March 10, 2008

Enclosures:

- Petition for Extension (2 Months); and
- Additional Claims Transmittal